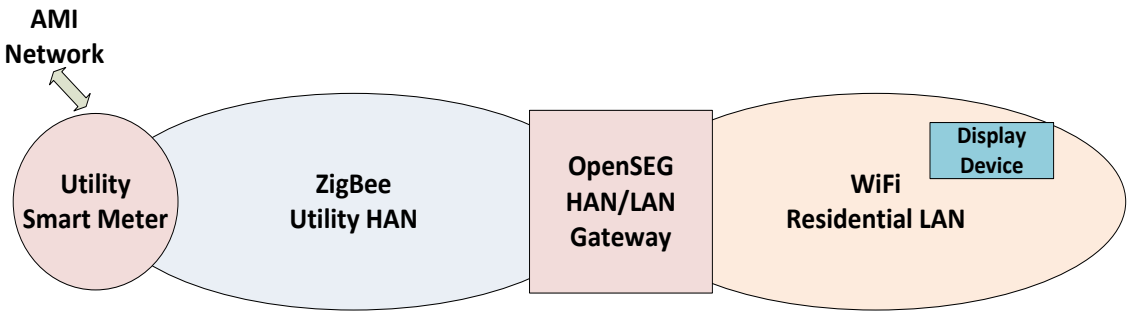
Specification for
Open Smart Energy Gateway (OpenSEG) Device

Introduction and Overview:

This software specification for a residential Smart Meter gateway device has been developed as part of the Residential Energy Display Survey (REDS) project at the Demand Response Research Center, LBNL. In the first phase of this project, our goal is to facilitate the display of near real-time energy consumption data within the home and to explore the usefulness of this data to consumers. Fundamental to achieving this goal is the ability to stream energy (power-consumption) data from the residential power meter to some form of in-home display. During this phase of the project, we will be focusing solely on existing in-home display devices (smart phones, PC's TV, etc.), thus demonstrating Smart Meter usefulness within the existing and immediate home environment. This basic capability, i.e. residential access to meter data, is considered one of the major and, hopefully, immediate benefits resulting from the wide-spread deployment of Smart Meter and Advanced Metering Infrastructure (AMI) technology in California over this past year – one which many parties are very motivated to publicly demonstrate. However, at this point in time, the usability of this Smart Meter capability is relatively unclear and the ultimate ability to provide data into the home from these meters remains yet to be demonstrated on any reasonably scale.



As a result, the REDS project has looked closely at the common issues (both architectural and policy) that are influencing the direct streaming of Smart Meter data into the home. Among California utilities, we have found there is a general concern about the level of security found in the current implementation of the SEP 1.0 (Smart Energy Protocol) which is used to communicate between Smart Meters and in home devices. When this uncertainty is combined with uncertainties about the level of maturity present in newly deployed AMI systems, which support wide area communications between utilities and Smart Meters, there remains little enthusiasm on the part of utilities for the wide spread enabling of Smart Meter Home Area Network (HAN) radios in the "wild". Many utilities are delaying activation of HAN radios until late 2012 (or later!) in anticipation of the increased security promised by the yet to be published SEP 2.0 standard. There are also several outstanding issues centered on the ease with which existing utility back office software environments can support deployment and registration of SEP 1.0 devices within their service areas. While these concerns are understandable, some degree of haste in demonstrating Smart Meter capabilities is considered prudent. We believe that, by adequately limiting the scope and type of SEP messaging permitted on the residential utility HAN, such a demonstration is possible – in the near term. Furthermore, we believe these existing networks can be used to stream near real-time meter data into the home with minimal

risk to either utilities or customers. This can be accomplished through the use of a simple and secure gateway device that, in a well understood and limited manner, allowing the movement of Smart Meter data through the utility HAN to the residential LAN (e.g. WiFi, Ethernet, GPRS, etc.) commonly found in current residential settings. The following "strawman" specification outlines the features and requirements of such a gateway and, along with further discussions, will enable vendors to implement gateway devices suitable for Smart Meter data streaming demonstrations. The gateway function defined in this document is expected to be absorbed into routers, set-top boxes, and other consumer-owned appliances in the future. However for this field test, special-purpose devices are anticipated.

Functionality:

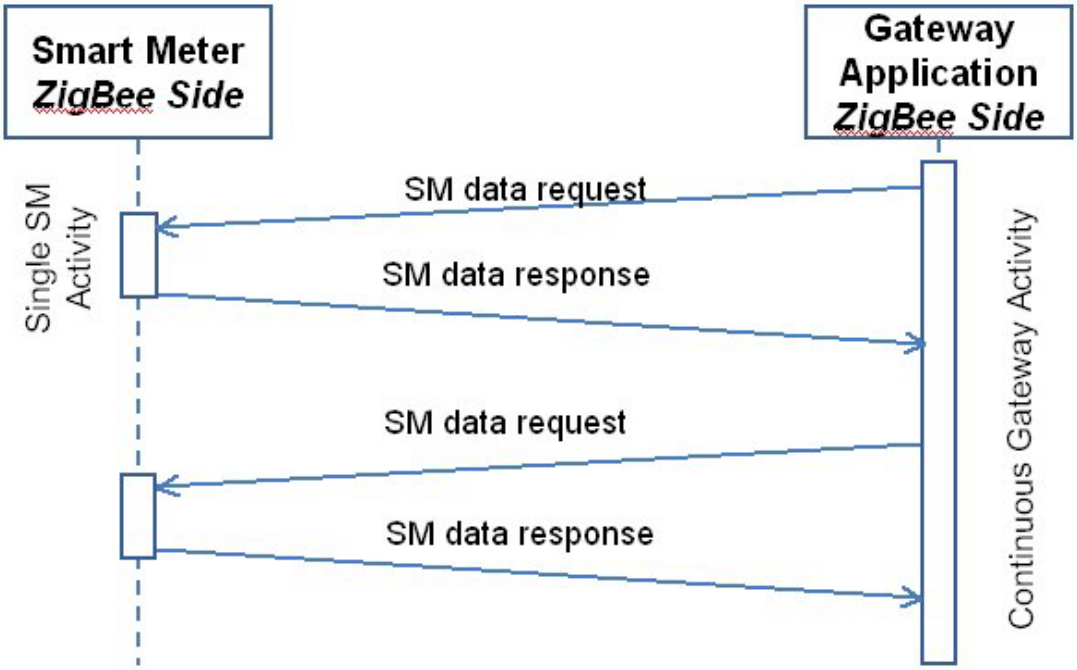
This device will function as a gateway between a utility-controlled residential HAN and a residential local area network (LAN). While much of this device's behavior is determined by its two required protocol stacks (Zigbee Pro and TCP/IP), the following specific application level functionality is required.

On the HAN side, the gateway will, upon receipt of a suitably formatted request (see below). query the Smart Meter for the value of two specific C12 table entries These entries will correspond to instantaneous energy consumed (i.e. kW) and current integrated power (i.e. kW-h) as seen by the meter's metrology circuitry. This data is currently found in all meters implementing standard C12 tables and is internally represented by a 48-bit binary value. The gateway will service and respond to such requests at a rates up to once every 7 sec. – as described in relevant ZigBee SEP 1.0 specifications. Data resulting from this query will be stored along with a time tag that will allow these values to accurately displayed in an understandable and correct time sequence by an unspecified display device/process. Absolute time accuracy for individual readings is not critical and may differ from actual time (e.g. that obtained via Network Time Protocol) by 30 to 40 sec. Time tag values associated with metrology data must have a consistent relationship to the actual time of measurement to within 1 sec. And relative time values for sequential measurements should be within 1 sec. of the proscribed query interval. There is no requirement that the gateway device provide capability for extensive data logging or the ability to query past readings.

In order to support these operations on the HAN network, the gateway device must be capable of discovering and/or requesting the Smart Meter network address. As the HAN coordinator, the Smart Meter is typically placed at address 0. The gateway must be able to verify this and, if incorrect, provide some mechanism for indicating that it cannot contact the meter. While the HAN protocol stack will be responsible for correctly responding to missed or corrupt packets, the gateway application must recover from corrupt or incomplete queries reported by the HAN stack. It should accumulate statistics for total and lost Smart Meter queries and indicate, by way of properly adjusted data time tags, the absence of a meter value for a given interval. With respect to the utility HAN, the gateway application should, once properly configured, initiate meter queries on power up and execute them, at suitable programmed intervals, continually.

In essence, the gateway application will support a subset of the read operations implemented in the SEP 1.0 Simple Metering Cluster" (ZigBee 1.0 specification, Document 075356r15, Annex D.3) Except for meter data queries and ancillary messages needed for device discovery, service discovery and support of a limited number of Simple Metering Cluster read operations, ,

no other SEP 1.0 operations are proscribed or allowed by the firmware executing this application. We are aware of several existing hardware platforms that are capable of hosting the application described here. While we realize that this application can, and hopefully will, be implemented on existing hardware platforms, the acceptance of this application design by utilities will largely depend on their ability to quickly and accurately determine the potential risk that a given implementation presents to operations on the utility HAN and, more importantly, the utility AMI network. Therefore, we suggest that, regardless of additional capabilities present on a given hardware platform, it be possible to disable all HAN activity except for those ZigBee Pro and SEP 1.0 messaging activities required by this application. This capability will further decrease accessible points of attack and provide enhanced HAN-side security by denying service for SEP 1.0 services that may not be fully implemented by current meter firmware.



On the residential LAN side, the gateway essentially acts as a web server that is capable of responding to properly formatted requests for meter data. These requests must be formatted as HTTP/REST web service requests over a suitably secured TCP/IP socket channel (see details below). Given the recent development of the Green Button Initiative, we have decided to make OpenSEG data available using published Green Button data formats and query semantics. Although the resulting Green Button-formatted data message will be appreciably larger than the smallest possible representation of meter energy and power data, the resulting flexibility and adherence to a widely known standard is felt to be beneficial.

In describing the role of the OpenSEG design as a source of Green Button data, it is important to understand the standard that served as the basis of the Green Button initiative. The ESPI-REQ.21 (NAESB) standard, which defines the underlying URI and data formats for Green Button messages, was originally defined for generalized data exchange between data servers and multiple authorized third party applications. It proposed a secure process by which end users could give specific third parties authorized access to their energy consumption data. As a result,

this standard developed authorization mechanisms intended for large, enterprise-like IT environments that differ from those found in typical residential settings. Therefore, we propose several accommodations in the use of this protocol that should simplify its implementation on light-weight embedded platforms.

First, this specification does not require a specific mechanism for the exchange of an Authorized Third Party ID. Authorized Third Party IDs, which should conform to the published Green Button specification, can be exchanged between the OpenSEG and client application through any suitable – and secure- out of band mechanism. For example, gateways and clieint applications can be manually configured with suitable IDs. Or, IDs can be based on client platform MAC or IP addresses.

Second, OpenSEG implementations are not required to provide historical data archiving capabilities. For example, an OpenSEG query using a URI with a well-formatted time interval parameter can, legitimately, return a simple "data not found" response because the ability to query for Smart Meter data from a previously sampled interval is considered optional. However, when queried for Smart meter data with a URI that *does not contain any time interval parameters*, all conforming OpenSEG implementations will respond with a single value that represents the current instantaneous value of the queried data value.

External Interfaces:

For the purposes of the application specified, the gateway has two primary external interfaces: the utility HAN and the residential LAN.

Utility HAN:

In order to provide the functionality described above, a gateway device must be able to join the utility HAN as a conforming Zigbee Pro and SEP 1.0 network device. This implies that the gateway has been fully certified by the Zigbee Alliance and has requested and received a production-level Zigbee SEP 1.0 security certificate from Certicom, Inc. It must be capable of being provisioned by the participating utility using their approved device installation procedure and be able to join and participate in their field-deployed HAN networks. Furthermore, to achieve enhanced levels of security associated with the reduced levels of functionality described above, the utility meter should only allow one HAN device, namely, the OpenSEG device, to be provisioned and join its Zigbee network. It also implies that the gateway device has application-level firmware that is capable of originating SEP 1.0 compliant queries for one or more elements of the Smart Meter's Simple Metering Cluster and successfully interpreting Smart Meter response messages.

It should be noted that, in practice, these capabilities can be non-trivial to implement and, as shown in the Texas "Go-To-Market" program, can require extensive testing effort on both the part of the vendors and the utilities. Since California, provisioning and device certification efforts are not as advanced as those in several other states (e.g. Texas, Oklahoma), it is difficult to explicitly specify requirements for acceptance by California utilities. However, since our project goal is to investigate the use of near real- time Smart Meter data, gateway devices must be accepted by participating utilities for use within their networks. If devices are not already formally (or informally) approved for use by participating California utilities, it must be clear that the efforts to obtain such approval are both reasonable and acceptable to staff at utilities, vendors and the REDS project team. A security testing laboratory at California State University at

Sacramento (CSUS) and well as an application testing laboratory at Lawrence Berkeley National Laboratory (LBNL) will be available to augment utility testing.

Residential LAN:

On the LAN side, this device must be able to function as part of a residential 802.3 (Ethernet) or 802.11 (WiFi) network. Given the relatively low expected data rates, minimal data rates for either of these media standards are adequate. The gateway must be capable of functioning with both static and dynamic IP addresses and be capable of auto speed negotiation (for 802.3 media) or acting as a secure (WPA2 PSK) wireless supplicant (for 802.11).

Relationship to Existing Standards:

The gateway implementation is expected to comply with a number of widely used standards needed to function in a modern LAN environment. Compliance with standards such as TCP/IP, HTTP, and HTML are both commonplace and necessary requirements and will not be enumerated here.

ZIGBEE SEP 1.0:

The gateway device will comply with published ZigBee Pro and SEP 1.0 specifications for all communications on the utility HAN side of the platform. Given the current state of these documents, demonstrated compliance (i.e. ZigBee certification) with these published specifications may not insure interoperation with all utility Smart Meters. As noted elsewhere, lab and field testing of gateway platforms with a given utility's SEP 1.0 implementation is the best, and ultimate, indication of compliance.

Transport Layer Security (TLS):

It is our belief that, once data leaves the utility HAN and enters the residential LAN, its custodianship passes to the consumer and its protection is no longer a utility concern. However, it is important to provide tools that will allow consumers to protect energy usage data within their own security domain – namely, the residential LAN. Therefore, the gateway platform must support TLS (Transport Layer Security) connections (e.g. HTTPS) for securing connections between the gateway and other nodes on the residential LAN. This will insure that, if desired, communications containing energy usage data will be encrypted at levels consistent with levels found in general e-commerce Internet transactions. Furthermore, to eliminate the potential for non-authorized clients to access the gateway device, transactions between the gateway device and an IP client must implement, subsequent to successfully establishing a secure TLS channel, the HTTP "basic authentication" scheme. This scheme requires client nodes to present a known, correct user/password phrase pair as part of the HTTPS/REST request. This technique is widely used in secure Internet transactions and is accepted as simple to implement and relatively secure. This mechanism will require IP clients to pre-registered user/password token pair with the gateway through an unspecified configuration or provisioning operation. Note, this specification does not require the use of client-side certificates to uniquely identify the requesting user. If required, user identity is verified through the combination of server-side certificates (via HTTPS) and HTTP basic authentication.

REST Web Services:

Representational State Transfer (REST) web services represent a simplified, light-weight methodology for implementing client/server web service transactions. Although REST services are built using standardized HTTP/1.0 elements, their syntax is not formally standardized.

Gateway REST web service implementations should be harmonized with existing "best practices" as described in appropriate W3C documents (e.g. http://www.w3.org/TR/ws-arch).

Green Button Initiative:

As described above, data formatting and query semantics between nodes on the residential LAN and the OpenSEG device will follow the patterns described in the Green Button initiative. Details on this specification can be found at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/GreenButtonInitiative. Additional information concerning the supporting ESPI-REQ.21 (NAESB) standard can be accessed at http://www.naesb.org/ESPI_Standards.asp

Performance:

Details of expected performance can be found above. But, in summary, the gateway platform and application firmware described here must be capable of continual, successful Smart Meter C12 table queries (through the SEP 1.0 Simple Metering Cluster interface) for a single table value at rates up to one query every 7 sec.

- Continual, successful Smart Meter C12 table queries for a single table value at rates up to one query every 7 sec.
- Respond to REST web service queries received from the residential LAN at rates of up to one query every sec.

Design Attributes:

With the exception of the two required protocol stacks, the functionality of this device is relatively simple – by design. However, there are several attributes that all successful implementations will share.

Robustness:

Once installed and in use, this device should operate continually and reliably without user intervention. If power to the device is lost, it must be capable of booting itself, rejoining the utility HAN and be capable of performing meter query operations (as configured) on the restoration of power to the device and/or the Smart Meter. If the functionality described in this document is shared with other device behaviors and functions (e.g. data logging to a "cloud" application), these functions must be implemented in a way that does not impair the ability of the device to continually perform the actions described here. In particular, functions not related to those described in this document should not impair the device's ability to poll the meter at well-defined intervals and respond to data requests from platforms on the residential LAN. While the co-exsistence of such feature may provide addional cyber-security risks, these are, for the purpose of this specification, considered out of scope.

It is not unlikely that the most complex software entities in this device will consist of the utility HAN and IP protocol stacks. Therefore, every effort must be made to insure that these two software components do not interact adversely with the functionality described above. Unbounded latencies and intermittent dropped connections can have unintended effects as higher levels which can be difficult to analyze and, ultimately, sacrifice the overall performance of the device.

Clear and Readily Understood Implementation:

This device has two primary functions. First, it continually acquires and caches power consumption data from a designated, nearby Smart Meter. And, second, it responds to IP-based requests for cached Smart Meter data arriving from the local residential LAN. Given the scope of the REDS project and the interests of its various participants, this device's functionality has been specified in a manner that promotes the separation of these two activities and minimizes the potential for unintended interactions with the utility HAN. Other than simple synchronization primitives that allow mutually exclusive access to shared data, a successful design must implement these two behaviors as separately-coded, sequential operations that offer minimal potential for corrupted overall behavior. While software specifications typically do not discuss actual implementation details, given the security concerns of all REDS participants, it is critical that the program code governing this device's behavior enforces this separation and, under analysis (visual or otherwise), clearly demonstrates its intention to do so. This can be accomplished through a number of structured coding and documentation practices that promote behavioral analysis. From a security perspective, the gateway application will follow the "only read from, never write to the smart meter" principle .At no time should the gateway application be permitted to transmit to the meter a SEP packet that will be interpreted as a "write" operation (as interpreted by any SEP cluster). Software tests that demonstrate gateway behavior on both HAN and LAN external interfaces at performance extremes will be of further use in demonstrating correct and secure behavior.

Design Constraints:

Physical:

There are no explicit constraints on this device with respect to physical size and power consumption. However, given the REDS project goal of demonstrating the usefulness of installed Smart Meters communicating to existing home display platforms, it is important that the device's physical configuration promote the future vision of a ubiquitous device that may well become a standard element of every household. For example, while it is possible to implement the above functionality in a general purpose desktop PC, such a device would be physically inappropriate.

Electrical:

Similarly, a prototype gateway device that consumes 60 – 100W (or greater) during normal operation would be an inappropriate implementation when exploring and demonstrating the role of Smart Meters in promoting residential energy conservation. Conversely, it should be noted that there is no constraint that gateway devices be battery powered. A battery powered gateway device may, in fact, prove unreliable given the unpredictable processing load – and subsequent power consumption - that may be presented by residential display platform interactions.